Asian Journal of Applied Science and Technology (AJAST)
Volume 8, Issue 2, Pages 128-137, April-June 2024

Exploring the Frontier of Password Cracking: Methods, Effectiveness, and Defense Strategies

Tejas kottarshettar[1*] & Dr. Febin Prakash[2]

[1]Student, [2]Assistant Professor, [1,2]School of Computer Science and Information Technology, Jain (Deemed-to-be University), Bangalore, Karnataka, India. Corresponding Author Email: 23mcar0151@jainuniversity.ac.in[*]

DOI: https://doi.org/10.38177/ajast.2024.8212

Article Received: 19 March 2024 Article Accepted: 25 May 2024 Article Published: 29 May 2024

ABSTRACT

The manner of attacker's behavior cannot be underestimated; hackers use simple traditional attacks such as brute-force and dictionary attacks as well as sophisticated algorithms including: Markov models, probabilistic context-free grammars (PCFG), and generative adversarial networks (GANs). These are one of among the most advanced approaches which utilize artificial intelligence and machine learning to identify the patterns in passwords, guess them and crack them. Markov models calculate transitions from one character state to another, so they estimate password guesses as a probability which is sampled from the distribution. PCFGs further advance the concept by making use of context-specific inputs for producing the passwords, and as a result it is possible to come up with the candidates who are balanced and have the contextually valid characters. Years ago, the CPA attack was considered the ultimate approach for password cracking. Today, GANs have taken their place, implementing adversarial networks that use them as generators to generate valid password examples. It is evident from the research that abusing users' habits and context during password cracking has been proved that it can lead to a tremendous speed gain of the cracking process. The crackers exploit here patterns in the behavior and environmental features and tailor the cracking strategies. Besides that, recurrent neural networks (RNNs) and convolutional neural networks (CNNs) are considered to be good options in password modeling as well, where the ongoing researches are devoted to the structures of neural network so that the guessing powers of networks can improve. These new approaches have demonstrated an improvement of at least 10-15% over the outdated ones, thus they are credible in forming the password cracking paradigm shift. Thus, for defeating such sophisticated threats, companies should take into account such robust passphrase policies, teach the user about safety of passwords and implementation of rigid access mechanisms. Educating people on cyber threats basics and development of the reasonable cybersecurity culture are the factors that provide the impact reduction of attacks based on users' behavior and contextual information.

Keywords: Password cracking; Brute-force attacks; Dictionary attacks; Markov models; Probabilistic context-free grammars; Convolutional neural networks; Generative adversarial networks; Recurrent neural networks; Cybersecurity; User behavior.

1. Introduction

Cracking passwords refers as a broad range of techniques starting which includes the brute force till the advanced methods like Markov Chain Models, PCFG, and GANs which use an access to machine learning to predict the passwords. Markov models deal with character sequences to produce the more believable password guesses, in particular, hacks for complicated passwords. PCFG goes even further by considering a password syntax, and from the balanced ones password candidates are then generated that have a high chance for success authentication. Often, GANs, the latest breakthroughs in the area of the bypass tech, construct veritable dams to the entry of the system by means of imitating human-like passwords. With such scheme of things, they either employ generator that generates fake passwords or discriminator network that tries to distinguish between real and fake passwords, which make it impossible to defend against them [1].

Data analysis revealed that having two things: a user's personal data and context, will help recreate a password very quickly. The other point is that they are not happy with the way people formulate strong passwords which are not frequent. This may be recurring and a few members of the public could be scammed while others may learn and adapt to the mistakes that might spring up as a result of cyber crimes. Password-based brute force is an illegal attack on related passwords by hackers creating some from the online user's posts and social media access. This point actually refer to that the team just uses ready hacking bots to do the job. A backdrop of the activities of neighbors and institutions in the main monotonous life of private unimportant tasks will form a key component for the mission to be achieved. The turning point is the enemy not realizing that their plan was shattered and they had to come with a new plan based on shape-shifting. Therefore it yields a rise in the statistics of success. Statistics, the killers for cyber security, gives a function of hackers' indication in decryption, which means the developers should use better defense or strategy since cyber war shows never ends. To minimize the chance of risk selected organizations should develop complex password policies, create awareness about the eventualities & adopt latest authentication methods such as two-factor & fingerprint identification. A system full of teaching of cybersecurity constantly and selective data sharing helps to make sure that the attacks on the behaviors and context data are not so much [2].

It has been proven that the integration of machine learning with user habits and context facilitates the fast execution of password cracking. Attackers take advantage of the predictable behavior patterns, like using birthdays or family names grabbed via social media and online activities, to increase their success rates. Additional information, like job roles or the hobbies, adds to impersonation of the known climate that makes the victim more vulnerable. Through user profiles and context, cyber threats get more looming leading to the stringent defense system i. e strict security protocols, user education, and advanced verification systems such as multi-factor authentication. Additionally, bringing out data protection and ethical cybersecurity practices builds a guard against attacks that can use human behavior and context to their advantage [3].

The increasing application of neural networks, especially deep learning networks, to password modeling is something that has been widely acknowledged even by researchers. These networks have the potential to unlock the complex puzzles of passwords so as to increase guessing probability. Nonetheless, innovation of networks to raise the network complexity for effective performances should be pursued. Neural networks reproducing human brain's architecture get the data processed and make forecasts. They are capable of learning patterns and connections in passwords from multiplied datasets. LSTMs or RNNs, which represent the state-of-the-art in handling sequential data, are often employed for this purpose. Besides, CNN can also be utilized for cracking passwords because of its main benefit as a spatial pattern recognition. Instead of regarding passwords as sequences or texts of pictures, CNNs can actually learn crucial representations that aid making successful password prediction [4].

This way, they defeated the brute force virus that just needed time the efficiency of which was 10-15% more than that of regular password crackers. Considering advent of neural networks and enormous number of combinations (permutations) of passwords and being fed into the system, the neural networks will discover the invisible bonds (connections) beyond the principles of these traditional systems. It will show the features of adherence to be higher level pertinence (relevance).

Firstly, deep learning can uncover the password relationships of that and you will provide an opportunity to be prepared as if this happens, you can predict the next condition. Amongst the other techniques Markov chains, PCFGs and GAANs can be used for authority verification, passwords training and generation of real passwords. To accomplish the purposes of imitation and unauthorized login blocking, the experts present Markov models and PCFGs by mimicking the statistical feature recognition techniques, while GANs work through the implementation of adversarial training for replication of a legitimate one. What is important to note is that cracking methods are also getting more refined and they produce opposite result do to the fact that their power was limited in the times where this experiment was carried out. Businesses have to always accompany their cyber threats with new security measures such as tighter security protocols or password combinations when there is a new use of the old type or new type of attacks [5].

1.1. Study Objectives

(i) To give an insight about the existing and the new cracking techniques like the traditional technique of brute force and dictionary attack, the advanced techniques like Markov model, PCFG and GAN attack.

(ii) To measure the success rate of these password cracking techniques and the extent to which they can take advantage of users' behavior and other factors.

(iii) Gain insight into the feasibility of using such neural networks models as the recurrent neural network (RNN) and the convolutional neural network (CNN) in password modeling and cracking.

(iv) To unearth this information, we will discuss strict password policies, user education, and multi-factor authentication as some of the defense mechanisms against the advanced password cracking attacks.

(v) Cyber attacks that exploit human behavior and context knowledge need to be avoided and therefore there is need to build and enhance practicing of cybersecurity ethics.

(vi) In order to determine, whether the more sophisticated methods of password cracking are more effective than traditional techniques and, therefore, what their influence on cyber security measures might be.

2. Literature Survey

The researchers' have examined several various strategies aimed at overcoming the CAPTCHA in text-based form. They have classified this work into two main categories: single-view and multiview learning. In single-view learning, approaches applied are cognitive as well as artificial neural networks of which CNNs and RNNs, especially LSTM networks are. They are used to accurately understand the text of single-view CAPTCHA. The multi-view learning which entails using different angles to examine CAPTCHA sample images is a method that is used to improve robustness and precise. This would involve the implementation of different methods such as multiview CNNs and adversarial multiview learning which would be used to integrate information from different views or develop adversarial examples in an effort to better sign recognition. The diverse system for this CAPTCHA circumventing implies a four-step strategy to implement. Which allows is to do first is to get data about the different CAPTCHA images. It pre-processes the images by reducing size, normalizing, and compares the results with those ones obtained from the original image. Subsequentially, for instance, the CNNs and RNNs which are used for training the model with preprocessed data. And as the final step, the models are evaluated on a completely independent test dataset to obtain the estimation of the reliability and stability of their forecasts. This structured approach is intended for pointing the weaknesses of the typical CAPTCHA-based security mechanisms, so that better algorithms will be developed for solving the character-based CAPTCHAs [1].

Markov models and PCFGs make a strong point regarding the research methods in password security, applying a statistical approach to unravel the inscrutable patterns of passwords by character transition or character groups assessment. As aid, PassGAN is a very important advancement that uses the Generative Adversarial Networks (GAN) to enhance the password strength checkers on the internet. Through the training process on a real-world password data set, PassGAN creates very realistic candidate passwords which will result in a more robust rate of password strength evaluations, and in the end, the security measures will be well protected against adversarial attacks. Such developments are a testament that deep learning and probability of statistics are in the process change how security of passwords is done, signifies continual efforts of protecting the confidentiality in cyber security [2].

The process of password cracking and analyzing user behaviour entails revealing such important information as weaknesses of cybersecurity systems. The methods, such as brute force and dictionary techniques, on the one hand, and advanced techniques like Markov models and probabilistic context-free grammar (PCFG), on the other, when analyzed by researchers, yield a holistic picture of intrusion tactics utilized by malicious users. User habits as far as password selection requires more attention; people often choose easy-to-guess phrases or add in personal data creating a leeway for password exploitation.

Furthermore, understanding the importance of the context in making a password and a hash of it is the key. The needed data can either be from social media where personal details can be known or knowledge of an organizational dynamics. The data can be effectively used at cracking. Using the human factor, the hackers may enhance the effectiveness of phishing actions or find cracking loopholes that exploit individual user actions. This emphasizes on the need for context-sensing password security procedures which would ask organizations and individuals to establish strong authentication mechanisms and help users understand the dangers of simple passwords. As cyber threats evolve, contextual thinking should be a prerequisite for endurance of protection strategies that are aimed at the repelling of the most sophisticated attacks [3].

Investigation of randomness leakage vulnerability in lattice-based Fiat-Shamir cryptographic signatures is the main lesson from this. Such a case where the trusted protocols are breaking down calls for very intense examination. Scanning the risks of randomness leaking within the lattice-based Fiat-Shamir signatures, the researchers boast to detect flaws in security that may make the cryptographic systems to intimate and unsafe to the users. From this, a recovery attack with similar leakage but of a minimal randomness is presented as one of our main contributions. The attack does take advantage of the unnoticed disclosure of small randomness by the cryptographic protocol which remains undetectable. This random disclosure of which is termed as the leakage enables the attacker to recover the secret keys and hence the security of the system has been violated. Researchers therefore particle in the perpetual activity attempting to fortify the cryptographic protocols and bolster against all kinds of attack. This investigation illustrates the importance of preemptive security analysis and constant improvement of cryptographical implementations serving the purposes of maintaining with the digital world the confidentiality, integrity, and quality of communication and transactions in the space of data and information exchange [4].

In the field of cybersecurity, the presence of backdoor attacks in Natural Language Processing (NLP), where nearly imperceptible triggering mechanisms or patterns are implanted into learning algorithms but remain dormant until a particular input is made, is an issue of paramount consideration as it can potentially result in mischievous outcomes. To address this risk, strategies like robust training techniques, adversarial training, and model verification methods have been developed in order to increase model resilience and reliability, making sure that NLP systems cannot be easily distorted. Furthermore, in intricacies of computer vision various invisible triggers and attack methods comprising of adversarial attacks and stealthy manipulations are investigated to disrupt the vision recognition systems. Adversarial training as well as sanitizing input are the two defense strategies that defend the system against such threats with the goal of improving the robustness and security of computer vision applications [7].

3. Fundamentals of Password Cracking

3.1. Password Encryption vs. Hashing

(1) Encryption: It is as if you are trying to decode a message but you also have to uncipher it with a key. First of all, the original password (plaintext) becomes ciphertext by using encryption algorithm and a secret key. To unscramble the code and open the data, you have got to have the receiving end as both the ciphertext and the key. Secondly, Providing for password recovery in the entity’s will, if encrypted, is possible only when having the key available, which is rather not applicable for a secure system.

(2) Hashing: We cannot return the food waste to the original form. The password is consumed by the hashing function, which consequently creates a distinct string of letters (hash). It's more or less like creating a fingerprint for the password. To your positive, in contrast with fingerprints, you remain unable to reach the real password from the hash. For this reason only password hashes are stored in the webs and not the original credentials without the hash.

3.2. Password Cracking Attacks

Here are some common types of password cracking attacks. Here are some common types of password cracking attacks:

(1) Brute-Force Attack: This approach in turn brutally operates the all possible symbols mixtures until the password is found. Its multi-stage processing is fine for long and complex password but for short and simple it is slow.

(2) Dictionary Attack: Thieves’ strategies include working with a catalog of default words, phrases and common word mixes. This also entails addition of leaked passwords from earlier security breaches to their guesses. On the other hand, the second attack is more rapid but is less efficacious for the old-fashioned passwords.

(3) Hybrid Attack: It consists of the combination of both patterns of brute-force attacks and dictionaries, often composing passwords. First, it will surely give you simple words and then in future, it will use numbers and symbols to increase the further complexity.

(4) Rainbow Table Attack: Looking-up-tables store already traced passwords which have corresponding hashes. Attackers extract the password hashes from stolen source files to check if the hashes have corresponding entries in the rainbow tables. Nevertheless, running and sorting these tables is a challenging task to be done in the limited resources.

(5) Social Engineering: Through this trick, it has hit the bottom line of users' psychology and caused them to lose their passwords. Phishing mails, fake log-in pages and shoulder surfing are the examples of social engineering which coerces the victims to give up the sensitive confidential information.

4. Defense Mechanisms and Mitigation Strategies

A multiview deep learning system is an architecture that has used several viewpoints instead of a single one to improve its learning effectiveness. For the image classification problem, multiview deep learning system will be involved with the use a view of an image, such a color channel and image transformation, to enhance the accuracy and robustness. A twofold approach of using Convolutional Neural Networks (CNNs) and repeated networks (e.g., Recurrent Neural Network or RNN) on multipoint deep learning system enables a heuristic way of modeling spatial and temporal information, which are complementary variables in myriad types of analysis. CNNs manage to capture spatial patterns better comparing to other techniques. So, these are good for image recognition.

However, recurrent networks including LSTM are efficient in processing temporal data as well as capturing relationships within such data. The system combines CNNs with recurrent networks, and it thus capitalizes on the complementary strengths of each architecture. CNNs examine spatial features from data input, internally extract relevant patterns and representations, while recurrent networks carry out sequential or temporal features analysis, therefore, catching context and dependencies between data elements over time. Through such coalescing the system effectively amplifies its power to sort out complex data precisely, notably when there are both spatial and temporal data involved [1].

In order to change the cost function to an RNN-based one we adapt a loss function specifically for Recurrent Neural Networks (RNN) which is that of sequential data processing tasks. Unlike the traditional cost functions like mean squared error (MSE) or cross entropy, the cost functions of RNN are specifically tailored to model sequence-related dependencies or long-term structure in sequences. Technics such as sequence-to-sequence loss and reinforcement learning objectives are used to improve the efficacy of the RNNs in tasks like language modeling, machine translation and time series prediction. The cost function adaptation to a task, specific sequential data properties and requirements allows RNN-based models to be trained better, which, in turn, results in higher accuracy and performance. Using dual-discriminator GANs widens the horizon of ability of GANs by incorporating two discriminators instead of one. These dual discriminators possibly impact differentiable in terms of captured data, thereby refining the process for the generator. As for instance, in image generation cases, a discriminator could assess high-level features like object shapes and the other one could evaluate low-level textures. Thanks to the dual discriminators, GANs can give more detailed comments and feedback that in turn improves the variety of samples generated across different fake domains like image generation, text generation as well as data synthesis. So far, this approach has led to the state-of-the-art models in most of the machine learning and AI tasks. This shows how dual discriminator GAN structures help to improve generative modeling performance [2].

Dictionary attack custom dictionary generates the tailored wordlist (dictionaries) that has been developed by a specific condition. In contrast to the usual wordlists that include commonly used passphrases or words, a custom dictionary is created and tailored to contain relevant terms to the desired organization; these may be company or product names, industry-specific terminology, or employee-related information. Such lists could additionally have patterns figured out from earlier breaches done or public data sets with target organization, thus giving with a higher chance of cracking password procedures success. By personalizing the dictionary to meet the particularities of the target language and the context where the password is being used, the attackers will have better chances to discover the password which will later help them to penetrate accounts or systems.

In addition, implementation of information gathered from surrounding situations of the investigation in the methodology of password cracking technology raises its effectiveness, as it provides unique access to data on habits and preferences of users. This contextual information can be patterns of password creation, user specific statistics or organizing structure, and industry-based norms. The investigation of this contextual information enables the attackers to adopt their attack plans according to the nature of the target environment and raise the productivity of their attempts in that respect. Furthermore, in the event context, it could be possible to find a way to breach password security that might have been done wrongly so as to facilitate attackers exploiting that vulnerability more effectively. To sum it up we can say that the custom dictionaries and contextual information obtained play a major role in the success of the attempts for password cracking because it is necessary to have the knowledge of the environment and the characteristics of the target in the case of cyber operations [3].

Generic key recovery attacks aimed at recovery of secret keys from a cryptographic system with minimum randomness leakage are the cryptographic attacks that aim at recovering the secret keys with a minimum amount of randomness leak while they are being attacked. These kinds of attacks usually are carried out to target systems where the creation of random values is a basic to cryptographical algorithms used in securing networks. The attackers try to decrease the exposure and take advantage of a weak cryptographic system to increase the possibility of successfully cracking the system. Another method of the opposite process presents the non-profiling attacks of power error of polynomial addition. Addition of polynomials in many forms of encryption algorithms as well as in modular arithmetic is one of very common. These exploits are likely to take the form of alterations, or compromising of secret or key values, which are among the most enticing targets for attackers to recover these keys.

To perform Power Analysis Attacks, multiple development factors are exploited that include variations in device current or emission of electromagnetic waves. Through constant monitoring of these dynamics, hackers will try to indirectly interpret information about the internal status of the device which can be sensitive such as secret keys or intermediate values in the process of cryptographic operation. When it comes to polynomial addition operations, power analysis approach can be used to detect links or correlations between power consumption and values being processed, ultimately enabling the security of the secret keys in r=1 oblivious computation with limited risk of randomness leakage. Assailants now rely on the combined use of power analysis for polynomial addition purpose to achieve their nefarious designs. This enables attackers to bypass the need of in-depth profiling of their targets or even in the knowledge-based acquisition of cryptographic information. Consequently, it makes the ordeal more versatile and applicable to a wide range of cryptographic gadgets and implementations. This form of attack pinpoints the need of elaborating countermeasures like secure hardware design, resisting side-channel attack and employing randomness protected mechanism to deter key accessibility which may ultimately lead to the compromise of cryptographic systems and the average user privacy against the sophisticated adversaries [4].

Particularly, Markov models and Probabilistic Context-Free Grammar (PCFG) are involved in the password guessing strategies searching of passwords using the statistical patterns and rules of the context. Markov models work in a manner that detects character transitions while at the same time learning from the observed patterns discovered in password datasets with a view of making the likely password conjectures. Likewise, the possibility exists that after realizing that "123" often follows "password" the model may therefore put emphasis on producing passwords that include this sequence. PCFG models take this feature further by comprising of syntax and structure rules which makes them suitable to develop novel and contextually relevant passwords. They determine the syntax of passwords, which involves the use of upper and lower case characters as well as special characters by analyzing statistic patterns. Despite the fact that Markov and PCFG models are powerful, there are still some limitations that may arise while trying to capture the highly complex patterns of the modern password schemes which use advanced strategies to improve the security level.

In the meantime, the neural networks, specifically the Recurrent Neural Networks (RNNs) and Long Short Term Memory (LSTM) networks also demonstrate huge potential in password cracking tasks as they can deal with sequential data very well. These networks exploit sequentially of passwords and can grasp distal connections and convey contextual information in passwords. Researchers devote themselves to improving the architecture of RNNs or LSTMs in order to achieve higher accuracy and efficiency when tackling password guessing tasks.

Also, newly developed architectures of artificial neural networks, and include the isolators, and the transformers, seek to stretch the boundaries of guessing the passwords' accuracy. Attention mechanism supports a network to process a sequence of denoted factors correctly which makes learning more efficient thus enhances the performance of the tasks having long range dependencies. Transformer models have produced outstanding achievements and provide savoring experience in natural language processing tasks. This advancement can be pretty useful in guessing passwords by discerning the sophisticated patterns and roadmaps the passwords contain. The cooperative work is defining an effort aimed improving the derivation of passwords and at the same time enhancing the security of system passwords. Researchers attempt to improve the robustness and effectiveness of password-cracking methods with the assistance of different Markov models, PCFG models and neural network models, hereby also contributing to the security needs of the global community [5].

Convolutional Neural Network (CNN) is a unique architectural design for neural networks that addresses problems with image and video analysis. At the same time, attention-based Recurrent Neural Network (RNN) allows to integrate the mechanism of attention into traditional models of recurrent neural networks. CNN (convolutional neural networks) that borrowed the idea behind visual cortex of a human brain comprises of convolutional, pooling and coupled layers which allow automatic features based on images for tasks like an image classification. However, on other side to them, attention-based RNNs extend traditional RNNs, allowing the model to pay some special attention to specific parts of input sequences. Through this, the capture of long-range dependencies in tasks like machine translation and text summarization is improved. Both architectures are illustration of the deep learning applications to be versatile where the network can be used be for different domain applications with success [6].

5. Conclusion

The password cracking has undergone an incredible transformation using the substitution of primitive techniques by way of complex algorithms that leverage Machine intelligence and Artificial intelligence (Machine intelligence and AI). Markov models, PCFGs and GANs are in fact on the tip of the iceberg when it comes to the use of statistics, context-sensitive rules and adversarial models to create guesses which are realistic. As one of the most innovative tactics of cracking, algorithmic adoption of user habits and contextual knowledge is incredibly powerful that has indeed taken the cracking performance one step higher by ability to goal the attacks precisely at the individuals and environment the attacks are going to occurring. For example, neural network, including RNNs and CNNs, have shown to have potential in inviting creation as they are under active research to upgrade their layers for more accurate prediction.

And though they may suffice on a temporary basis, the fact remains that more resistant approaches need to be in place if current cyber-threats are to be kept at bay. Organizations must prominently emphasize on strong passphrase guideline, use education materials and deploy security measures like multi-factor authentication and biometric identification. In addition to it, a cybersecurity culture and sparring the alertness to security ideas are essential to resisting against human flaws used in the unauthorized access to the contextual data. Basically, the implementation of these advanced tools amidst the cyber space implies a steady demand for monitoring and reshaping in cybersecurity policies. Since updated and reliable security systems are vital for digital asset preservation, security identity, and safety in the progressively complex security environment, organizations must always evolve and be one step ahead of cybercriminals.

6. Future Suggestions

(1) Enhanced Neural Network Architectures: Subsequent research works should therefore endeavor to establish the creation of other enhanced models that involve more complexity in the construction of the neural networks, for example, transformers architectures that can help deal with complexity in password systems, in order to achieve higher cracking rates.

(2) Context-Aware Security Systems: Set persistence strategies capable of factoring the user movements and other related contexts to look for risky moves and eliminate threats.

(3) Integration of Quantum Computing: Find out if quantum computing can be of assistance in introducing new superior forms of securing data and systems or is it used to offset the severity of the current password breaking techniques.

(4) User-Centric Cybersecurity Education: Stress user related measures in cybersecurity teaching in an effort to share knowledge among individuals to understand what constitutes strong passwords and the repercussions of falling prey in social engineering frauds.

(5) Development of Advanced Biometric Systems: Design new technology more better than the passwords alone: make efforts in developing the required software/hardware for efficient deployment of biometric systems.

Declarations

Source of Funding

This study did not receive any grant from funding agencies in the public, commercial, or not-for-profit sectors.

Competing Interests Statement

The authors declare no competing financial, professional, or personal interests.

Consent for publication

The authors declare that they consented to the publication of this study.

Authors' contributions

Both the authors took part in literature review, analysis and manuscript writing equally.

References

[1] Yusuf, M.O., Srivastava, D., Singh, D., & Rathor, V.S. (2023). Multiview deep learning-based attack to break text-CAPTCHAs. International Journal of Machine Learning and Cybernetics, 14(3): 959–972. doi: 10.1007/s13042-022-01675-8.

[2] Nam, S., Jeon, S., Kim, H., & Moon, J. (2020). Recurrent GANs Password Cracker for IoT Password Security Enhancement. Sensors, 20(11). doi: 10.3390/s20113106.

[3] Kanta, A., Coisel, I., & Scanlon M. (2022). A Novel Dictionary Generation Methodology for Contextual-Based Password Cracking. IEEE Access, 10: 59178–59188. doi: 10.1109/access.2022.3179701.

[4] Liu, Y., Zhou, Y., Sun, S., Wang, T., Zhang, R., & Ming J. (2021). On the Security of Lattice-Based Fiat-Shamir Signatures in the Presence of Randomness Leakage. IEEE Transactions on Information Forensics and Security, 16: 1868–1879. doi: 10.1109/tifs.2020.3045904.

[5] Li, H., Chen, M., Yan, S., Jia, C., & Li, Z. (2019). Password Guessing via Neural Language Modeling. Machine Learning for Cyber Security, Pages 78–93. doi: 10.1007/978-3-030-30619-9_7.

[6] Zi, Y., Gao, H., Cheng, Z., & Liu, Y. (2020). An End-to-End Attack on Text CAPTCHAs. IEEE Transactions on Information Forensics and Security, 15: 753–766. doi: 10.1109/tifs.2019.2928622.

[7] Fanchao, Q., Yuan, Y., Sophia, X., Zhiyuan, L., & Maosong, S. (2021). Turn the Combination Lock: Learnable Textual Backdoor Attacks via Word Substitution. In Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing, Volume 1, Pages 4873–4883. doi: 10.18653/v1/2021.acl-long.377.